Mobile Access by dormakaba

White Paper for IT-Security Managers

Security for Mobile Access

dormakaba

In General

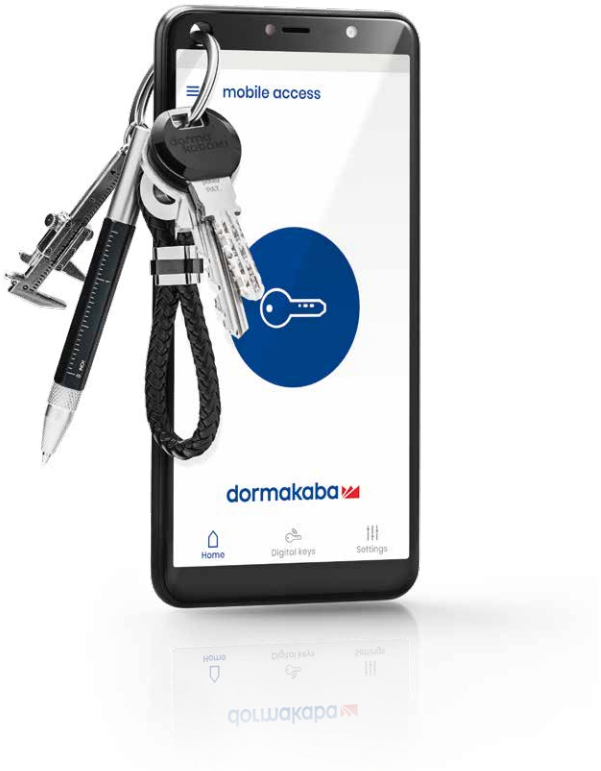
Advantages of Mobile Access

With Mobile Access, you can open doors with a smartphone. The smartphone therefore extends the range of access media consisting of keys and ID cards with RFID.
Access rights can be transferred to a smartphone independently of location and time. If a person is standing in front of a closed door, access permission can be granted to that person immediately, without having to hand over a physical medium (key, ID card). This also saves time and costs within the workflow.

Audience of this document

This document is specifically intended for the following users of the system:

- IT Security Managers



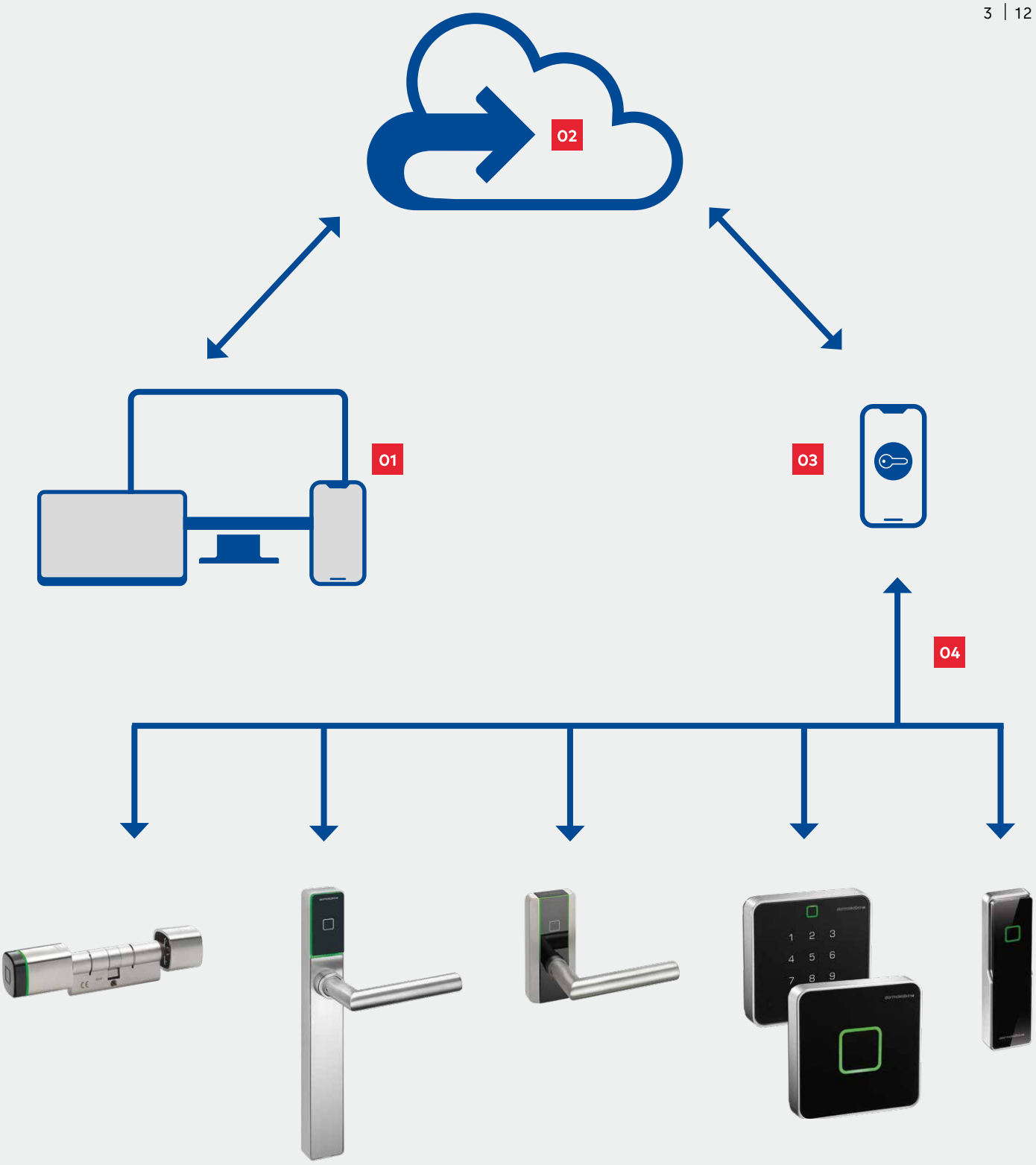
Structure of this document

The description of the contents of this document is divided into two sections:

- **Mobile Access Security Architecture:**
  This chapter provides an overview of the basic safety concepts and describes the relevant safety aspects as an introduction or overview.

- **Specific questions about security from the point of view of the IT Security Manager:**
  In this section, potential questions relating to the topic of security are posed and answered, so that the different aspects can be viewed from different perspectives.

Specific information can be found both in the overview chapter and also as answers to questions (sometimes to several questions). This means the information is sometimes available in several places. The redundancy of this information in the document is consciously accepted in order to be able to summarize the necessary information in the overview section as well as provide the appropriate answers to all questions directly.



Door components supporting

Mobile Access from dormakaba

Mobile Access from dormakaba consists of the following door components:
In the access solution **(1)**, access rights are assigned by generating digital keys, which are transmitted directly to the relevant smartphones via a secure platform **(2)**. With the smartphone and the dormakaba mobile access app, access is thus possible at the door components **(4)**. Communication between smartphone **(3)** and door component **(4)** can take place via NFC (Near Field Communication) or Bluetooth®.

Mobile Access Security Architecture

LEGIC technology is used for the secure transmission of digital keys. This enables encrypted transmission (interception and tamper-proof) all along the way:

- **from the controlling access solution**
- **via the cloud**
- **via a smartphone**
- **to the evaluating door component.**

End-to-end encryption

The central element is end-to-end encryption of the information (digital keys) that requires protection from the cloud to the door component, in particular:

- Encryption in the cloud:
  - The required encryption keys are only available in the cloud (they are stored in a hardware-safe environment, the so-called Hardware Security Module/HSM)
- Transmission from the cloud to the smartphone in an encrypted manner:
  - the information is encrypted on the smartphone and decryption keys are not available on the smartphone, i.e. information (digital keys) cannot be read, evaluated or modified
- Transmission from the smartphone to the door component in an encrypted manner (explicitly when attempting to enter):
  - The LEGIC chip is located inside the door component and thus the decryption keys are in a protected area inside the door component. Decrypted information is temporarily used to decide access and then deleted.

Encryption/safeguarding measures are also used on the various interfaces:

- Access solution ⟷ cloud (LEGIC Trusted Service): Encrypted communication: HTTPS over TLS
- Cloud (LEGIC Trusted Service) ⟷ smartphone: Encrypted communication: HTTPS over TLS, certificate pinning
- Smartphone – door component (LEGIC chip): Mutual authentication with AES128 session keys, new session keys for each session

Keys for encryption/decryption

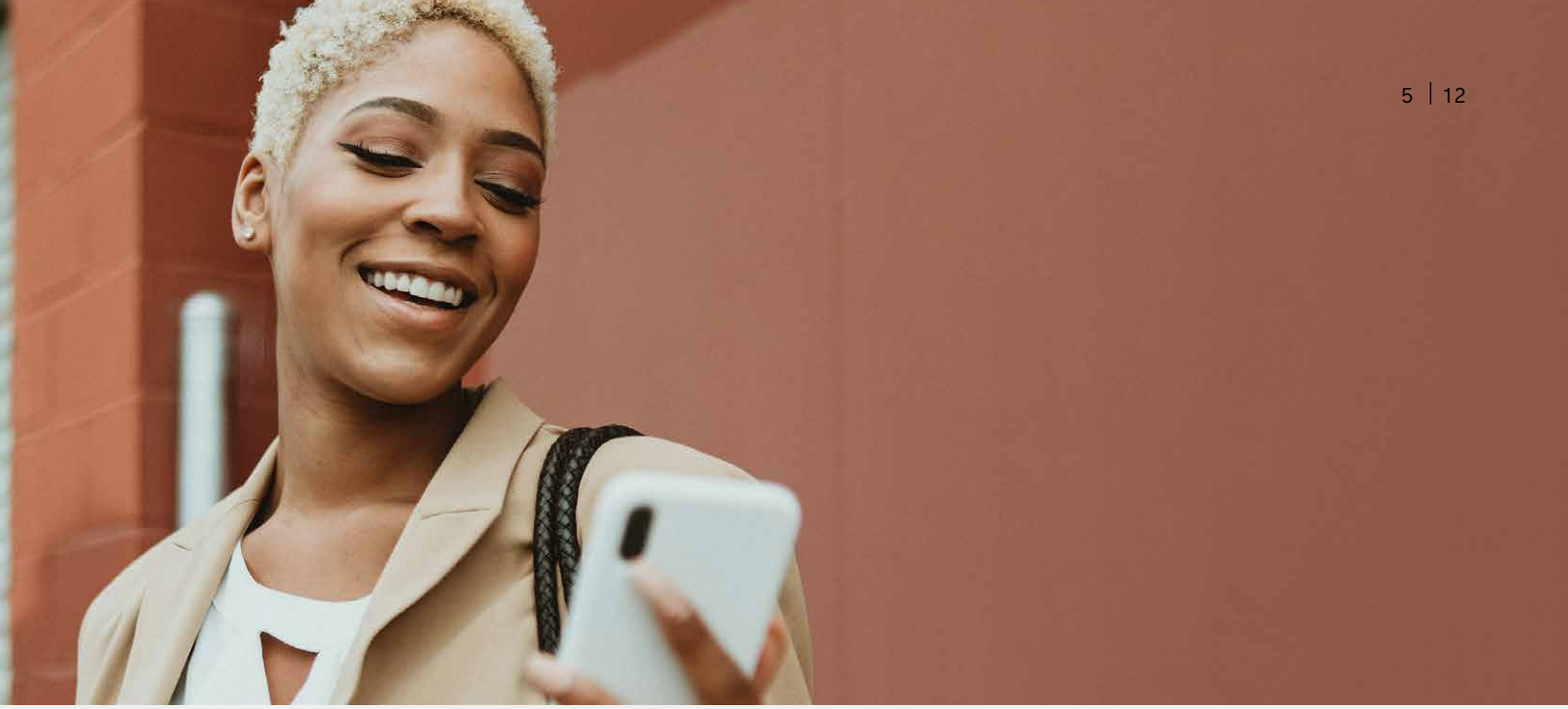
The keys for encryption/decryption are generated as random keys in the Hardware Security Module/HSM of the LEGIC cloud. The keys for encrypting and decrypting the information that is worth protecting (digital keys) are project-specific, i.e. specific to each installation. An installation typically covers company or site access control.
Project-specific use of the encryption/decryption keys allows the same digital keys for Mobile Access to be used consistently within an installation (e.g. within a company) (as is the case with RFID media). On the other hand, it prevents a company's digital keys from being used by another/independent company.

The keys for encryption/decryption are generated via the cloud (Trusted Service of the LEGIC platform), which securely generates these keys in a Hardware Security Module (HSM) in a certified security environment. These keys never leave the HSM in unencrypted form.

The required keys (for encryption/decryption) are transferred to the protected area (LEGIC chip) of the door component during commissioning. For this purpose, the required decryption keys are encrypted on the one hand and protected by various other security mechanisms and grouped in a so-called configuration package on the other hand. These configuration packages are transmitted independently of the access app via another app; this transfer is password protected.

Summary

- Random keys are used as keys for encryption/decryption.
- These random keys never leave the LEGIC cloud HSM in unprotected form (plain).
- For the transmission of the required keys, they are encrypted in a configuration package and protected by various other security mechanisms.



Types of digital keys

A distinction is made between two types of digital keys that follow different permission models:

- Infini-ID:
  Includes an identifying number for a smartphone/person; there is one per smartphone per project. The permission model with Infini-ID is particularly suitable for online readers and wireless components because the permissions can be directly updated on them (due to the existing online or wireless connections).
- Infinilink:
  Includes one person's access rules for exactly one door component. A person has an independent Infinilink key for each authorised door, which is visible in the dormakaba mobile access app.
  Infinilink keys have a limited validity period and are therefore updated by the controlling access solution in good time before the validity period expires (Infinilink keys with an extended validity). After the validity expires, access is not possible.
  The permission model with Infinilink is particularly suitable for standalone components because people carry the permissions with them and no manual updates to the standalone components are needed when access right changes are made.
  The blocking or deletion is done either by withdrawing the Infinilink key from the smartphone or by adding it to the blacklist of the door component.

Additional information on your smartphone

In addition to the contents of the digital key, more information from the access solution about the digital key is transferred via the cloud to the smartphone, which is not subject to end-to-end encryption. This information is encrypted on all relevant communication interfaces but can be accessed on the smartphone via the dormakaba mobile access app. Examples:

- Name of the digital key/smartphone number for Infini-ID or the door name for Infinilink
- Issue time of the digital key
- Digital key validity period (Infinilink), but not the detailed time permissions/rules of the encrypted digital key
- Company name

This additional information is used in the mobile access app to visualise information about the digital keys. The user can see this information for any digital key in the app. This additional information is not used for the access decision. This means that no change of permissions can be made by manipulating this information and, in particular, unauthorised access cannot be obtained.

Specific questions related to security from the perspective of the IT Security Manager

What encryptions are used between the different components?

The following specified security/encryption mechanisms are used on the communication interfaces between the various components involved:

- Access solution ⟷ cloud (LEGIC Trusted Service):
- Encrypted communication: HTTPS over TLS
- Cloud (LEGIC Trusted Service) ⟷ smartphone:
  Encrypted communication: HTTPS over TLS, certificate pinning
- Smartphone – door component:
  Mutual authentication with AES128 session keys, new session keys for each session

The digital keys for controlling access are end-to-end encrypted from the cloud (LEGIC Trusted Service) to the door component. To generate the keys for encryption/decryption, a Hardware Security Module (HSM) in a certified security environment of the LEGIC platform is used in the cloud (LEGIC Trusted Service)..

What data is transmitted via the interfaces?

The transmission of the access data (digital keys) between the cloud (LEGIC Trusted Service) and the door component containing the LEGIC chip is fully encrypted and the data is also stored in encrypted form on the smartphone. To select the file on the smartphone, there are further identifiers, which are transferred with the file.

Within the digital key is sensitive data, which is end-to-end encrypted as described in the previous sections. There is also other, non-sensitive data that is not transmitted end-to-end but encrypted on the respective interfaces.

The following data is transferred to the interfaces specified below:

Interface: Access solution ⟷ cloud (LEGIC Trusted Service)

- Digital key information (Infini-ID or Infinilink)
- Additional information about the digital keys for display on the smartphone, so-called LEGIC metadata (e.g. name of the digital key [for Infini-ID] or of the person [for Infinilink], issue time of the digital key, validity period of the digital key [Infinilink], company name)
- Access messages via smartphone
  interface: Cloud (LEGIC Trusted Service) ⟷ smartphone
- Digital keys (Infini-ID or Infinilink) – end-to-end encrypted
- Additional information about the digital keys for display on the smartphone, so-called LEGIC metadata
- Access reports via smartphone

Interface: Smartphone – door component:

- Digital keys (Infini-ID or Infinilink) – end-to-end encrypted
- Control information for the procedure (access with or without user interaction on the smartphone, ...)
- Status information of the door component, for display in the app (access granted, access denied, ...)
- Access reports via smartphone

Who opens the connection?

The connection between the smartphone and the cloud (LEGIC Trusted Service) is established by the smartphone, for example, to call up provided data.
The connection between the smartphone and the door component is initiated and controlled by the door component.

How is the connection secured?

Transmission and connections are secured in various ways:

1. Sensitive data (digital keys) is end-to-end encrypted, i.e. this data is continuously encrypted on the transmission path between cloud (LEGIC Trusted Service) and door component (LEGIC chip) and there is no key material on the transmission component (like the dormakaba mobile access app on the smartphone) in order to read, write or modify this sensitive data. The key material for encryption or decryption is only available in the cloud (LEGIC Trusted Service) and the door component (LEGIC chip) (see also the section End-to-end encryption).
2. In addition to the end-to-end encryption, all communication interfaces are secured/encrypted. On the one hand, this secures the transmission of less sensitive data, and on the other hand, it provides protection against various attack scenarios.
   - To secure/encrypt all communication interfaces, see the section What encryptions are used between the different components?
   - To protect against attack scenarios, see the section «Can I hack a digital key and gain unauthorised access?»

Is the connection end-to-end encrypted?

On the connection from the cloud (LEGIC Trusted Service) to the door component (LEGIC chip), sensitive data (digital keys) is end-to-end encrypted (see also the sections «End-to-end encryption» and «How is the connection secured?»).
The main reason for end-to-end encryption is that sensitive information is available in encrypted form on the smartphone. Decryption keys are not available on the smartphone, i.e. information (digital keys) cannot be read, evaluated or modified there.

How is the key transferred to the door component for encryption/ decryption?

The key material for decryption (or also encryption) is also encrypted from the cloud (LEGIC Trusted Service) to the door component (LEGIC chip) and additionally secured and transmitted on a second channel. See also the section «Keys for encryption/decryption».

How are the keys stored on the smartphone?

We distinguish between two types of keys:
- Digital key
- Keys for encryption/decryption

Digital key
Digital keys are stored within the app in an encrypted database. The digital keys are also encrypted differently per installed app (i.e. per respective app instance). This means that, even if someone manages to copy such a digital key, it cannot be used on another smartphone.

Keys for encryption/decryption
The keys used to encrypt or decrypt the digital keys are never passed to the smartphone and never stored there.
The smartphone uses only derived key material to secure the communication connection (NFC/BLE) to the door component. These derived keys are stored on iOS in the Key Store, and on Android they are currently distributed in encrypted form.

What is the safer communication technology between smartphone and the door component, NFC or Bluetooth®?

In general, the connection setup and the securing of the two communication channels NFC and Bluetooth® are identical, although NFC only runs over short distances and thus NFC connection is harder to intercept than BLE connection. In both cases, mutual authentication, new session keys for each session, are used as soon as a digital key (LEGIC neon file) is accessed. The connection is therefore secure, and only secured data is transmitted, which then can be evaluated for granting the access.
In addition to the digital keys (LEGIC neon file), other non-sensitive data is exchanged via messaging, which is not protected by the above mechanisms. Such non-sensitive data is used, for example, to enable convenience features. Also for this data, mutual authentication, new session keys for each session, are used on the NFC and Bluetooth® communication channels. An example is the status information of the door component for display in the app like access granted, access denied etc.

Can communication between smartphone and door component be intercepted?

Once the door component has established and secured a connection to read the digital keys from the smartphone, all communication is secured via individual session keys. Interception of the connection therefore does not reveal the transmitted encrypted content and cannot be used for replay attacks.

Can I hack a digital key and gain unauthorised access?

To secure the digital keys, a number of cryptographic backup mechanisms are systematically used, which prevent such manipulation. This prevents a digital key being hacked (i.e. decrypting and/or modifying the content).
The basic principle is the end-to-end encryption of digital keys (from the cloud to the door component), in particular, no keys are available in the dormakaba mobile access app on the smartphone for encrypting or decrypting the digital keys. This means that the digital keys cannot be modified (hacked) on the smartphone nor on the communication channels from the cloud to the smartphone or from the smartphone to the door component. However, not all attack vectors, such as copying a digital key, can be 100% excluded if an attacker already has access to the smartphone (rooted smartphone/jailbreaking), but the digital keys are subject to end-to-end encryption. The Mobile Access solution is therefore based on principles that ensure that each key is unique to avoid systemic attacks (‚man-in-the-middle', ‚adversary issuer', ‚replay' and ‚relay' attack scenarios).

How will protection be provided against ‚man-in-the-middle' attack scenarios?

To secure against ‚man-in-the-middle' attack scenarios, protection is provided on the following interfaces as indicated below:

- Access solution ⟷ cloud (LEGIC Trusted Service):
- Encrypted communication: HTTPS over TLS
- Cloud (LEGIC Trusted Service) ⟷ smartphone:
- Encrypted communication: HTTPS over TLS, certificate pinning
- Smartphone – door component: Mutual authentication with AES128 session keys, new session keys for each session

What is the protection against ‚adversary issuer' attack scenarios?

Use of end-to-end encryption, i.e. specifically no access to the sensitive data (digital keys) on the smartphone:

- Encryption of sensitive data (digital keys) in the cloud (LEGIC Trusted Service)
- No keys on the smartphone for reading/modifying/writing sensitive data (digital keys)
- Decryption (temporary) of the sensitive data (digital keys) in the door component for the access decision

How does the protection against ‚replay' attack scenarios take place?

Once the door component is authenticated to read the access permission (digital keys) from the smartphone, all communication is secured via individual session keys. Interception of the connection therefore does not reveal the transmitted encrypted content and cannot be used for replay attacks.

How can we protect ourselves against ‚relay' attack scenarios?

To protect against relay attacks, the digital keys on the smartphone are explicitly activated only for a short time and then inactivated again. When inactivated, the digital keys are unreadable and therefore not usable for a relay attack. Activation is an explicit action to be performed by the user on the app (button operation). After successful communication with the door component and the access decision by the door component, the digital keys are immediately inactivated. If no communication with a peripheral has taken place, the files will

be inactivated after a preset time has elapsed.
In the case of access with a smartphone without user interaction, the digital keys are not explicitly activated by the user, so in this case there is no protection against a relay attack. For this reason, it is recommended that the smartphone access scenario without user interaction only be used as a convenience feature in a protected area (e.g. office doors within a secured area) and, in the case of access in an unprotected area (e.g. entrance door), the access with smartphone scenario be used with user interaction.

Can my smartphone be cloned?

There is currently no cryptographic protection against cloning a smartphone. A prerequisite for such protection would be the consideration of a secure/unchangeable hardware feature for every smart device, which does not currently exist.
Securing against cloning of the smartphone is done exclusively at the app level:

- Infinilink keys have a limited validity, and access is no longer possible after the validity expires. The validity period thus determines the period of the potential vulnerability.
  The validity can be configured in the parent access solution; the shorter the validity period, the sooner an Infinilink key expires and access is no longer possible

Can a lost/stolen smartphone still be used for Mobile Access?

The protective mechanisms of the smartphone must be used to protect the smartphone against unauthorised use. Such protective mechanisms of the smartphone are, for example:

- PIN
- Fingerprint
- Facial recognition

These protective mechanisms already provide protection by the smartphone operating system against unauthorised use. For this purpose, the facility operator must adopt the appropriate technical or organisational measures or provisions.

In addition, the following options exist to prevent access to a lost/stolen smartphone if the protection mechanisms of the smartphone have been circumvented:

- Withdrawal of access permissions and thus the digital keys from the smartphone (via existing communication channels from the cloud to the smartphone)
  - The digital keys are removed from the smartphone by the parent access solution. It recalls the digital keys via the cloud (LEGIC Trusted Service) and thus removes them from the smartphone
  - The removal is successful if the smartphone is accessible (e.g. WLAN/Wi-Fi or mobile communication)
- If the smartphone is not accessible (e.g. no WLAN/Wi-Fi or mobile communication, or the smartphone communication is explicitly switched off: flight mode):
  - Infinilink: The app checks whether the smartphone has a functioning internet connection. If this is not the case for more than 24 hours, the smartphone user receives a corresponding warning message and can react if necessary (deactivate flight mode or activate mobile data or WIFI connection). If there is no Internet connection for more than 30 hours, the existing access rights on the smartphone are deactivated, the smartphone user is informed accordingly and requested to connect to the Internet. After a successful connection to the Internet, the access rights on the smartphone are updated and access is possible again according to the current access rights.
- Infinilink/Infini-ID: entry in blacklist of door components (via access solution)

How secure is the LEGIC cloud?

Access to the cloud service (LEGIC Trusted Service) is subject to authorisation management.
All instances of access solutions that use the cloud service (LEGIC Trusted Service) have an individual API key.
Communication is secured via https/TLS. Individual accesses to the cloud service (LEGIC Trusted Service) delimit the different instances.
There are organisational rules for accessing the cloud service by dormakaba (LEGIC Trusted Service) for service purposes.

What is the recommendation from a security perspective regarding the use of online readers, wireless and standalone components?

The permission model with Infini-ID is recommended for online readers and wireless components because the permissions on these door components can be directly updated (due to the existing online or wireless connections).
The permission model with Infinilink is recommended for standalone components because people carry the permissions with them and no manual updates to the standalone components are necessary when permission changes are made.
In the case of a suspected attack:

- For standalone components:
  - the smartphone must be accessible in order to remove Infinilink or
  - manual distribution of an entry to the blacklist is required or
  - it would be possible to access the door component up until the expiry of the validity of Infinilink.
- For online readers and wireless components:
  - Permissions can be revoked, blocked or blacklisted immediately without manual distribution.
  - Access can therefore be prevented directly

From a security point of view, the use of online readers and wireless components is therefore preferable.

What is the recommendation regarding the use of online readers, wireless and standalone components in different areas?

When using online readers and wireless components (with Infini-ID), there is the option of immediately withdrawing access permissions via the existing online or wireless connections.
When using standalone components (with Infinilink), there are various ways of preventing access in the event of a suspected attack, but these are less convenient or may also be blocked by the attacker.
This results in the following recommendation in order to combine security and convenience:

- Use of online readers and wireless components (with Infini-ID) on doors accessible from the public area (exterior); this underlines the security aspect at this point
- Use of standalone components (with Infinilink) on doors that are not in the public area, i.e. for which an access secured with online readers and wireless components (with Infini-ID) must have been passed previously; this underlines the convenience aspect at this point

This approach can counteract a potential external attack. For interior doors, standalone components with different convenience features can be used if a risk assessment allows.

Additional information

Term, abbreviation	Description
Door component	Generic term for online readers, standalone or wireless cylinders and door locks used for Mobile Access.
Access solution	Parent/controlling administration software application that manages access permissions, controls the transfer of the necessary configuration information to the door component and the distribution of digital keys.
NFC	Near Field Communication A transmission standard for wireless communication in the range of a few centimetres.
BLE	Bluetooth® Low Energy An energy-saving radio technology that can be used to network devices within a radius of up to 10 metres. Bluetooth® is a registered trademark of Bluetooth SIC Inc.
Digital keys	Electronic key, user-specific information on the smartphone that enables the door component to make access decisions.
Infini-ID	Digital key: Includes a number identifying a smartphone/person, which is evaluated for the access decision by the door component. Evaluation in the door component is carried out as a check against a quantity of Infini-IDs stored in the door component, if necessary with further access rules.
Infinilink	Digital key: Includes one person's access rules for exactly one door component. This access permission is valid for a limited time and must be renewed regularly (automatically) for continued access to the door component. The smartphone must be accessible for the update. After the validity interval has expired, access is no longer possible.
Blacklist	Quantity of Infini-IDs stored in a door component that prevent people with these numbers (Infini-ID) accessing this door component. By entering a person/smartphone number (Infini-ID) in the blacklist, access can be prevented even if there are other access rights.
Keys for encryption/ decryption	Cryptographic keys for encrypting and decrypting information (e.g. digital keys)

Term, abbreviation	Description
Random Keys	Keys for encryption/decryption, which are randomly generated in the HSM (Hardware Security Module), explicitly not manually generated (keys randomly generated in hardware security modules (HSM).
HSM	Hardware Security Module
‚Man-in-the-middle' attack scenario	Is a form of attack used in computer networks. The attacker is either physically or, nowadays, usually logically between the two communication partners, has complete control with their system over the traffic between two or more network participants and can see and even manipulate the information at will. The two-faced nature of the attacker is that they pretend to be the respective counterpart of the communication partners. See: https://en.wikipedia.org/wiki/Man-in-the-middle_attack
‚Replay' attack scenario	A replay attack is a cryptoanalytic attack on the authenticity of the data in a communication protocol. In this case, the attacker sends previously recorded data to fake a foreign identity, for example.
Rooted smartphone	Rooting a device with a Linux-based operating system, especially smartphones and tablets with the Android operating system, means creating extended rights for and by the user. These rights are also known as root or administrator rights. See: https://en.wikipedia.org/wiki/Rooting_(Android
Jailbreak (iOS)	Refers to the unauthorised removal of usage restrictions on computers whose manufacturer has locked certain features. See_ https://en.wikipedia.org/wiki/IOS_jailbreaking
IT Security Manager	The Information Security Manager is responsible for ensuring that all the assets, information, data, and IT services of a company are protected at all times in terms of confidentiality, integrity, and availability. They are usually part of an organisational approach to security management.

Any questions?

We look forward to hearing from you.

visit us:

Mobile Access Webpage by dormakaba

dormakaba International Holding AG
Hofwisenstrasse 24
CH-8153 Rümlang
T +41 848 85 86 87
info.@dormakaba.com
dormakaba.ccom